Boston Key Party CTF 2014 Crypto 100

原创

JDIIDJ 于 2014-03-06 12:29:31 发布 1354 收藏
分类专栏： CTF 文章标签： 密码学 计算机安全 CTF

版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。
本文链接：https://blog.csdn.net/jdisec/article/details/20618721
版权

CTF 专栏收录该内容
3 篇文章 0 订阅
订阅专栏

```
Mind your P's and Q's!
Crypto : 100

The flag has been split into several files, and encrypted under RSA-OAEP. Can you break ALL of the cipherte

http://bostonkeyparty.net/challenges/challenge-cd6d19866c42e274cd09604adaf4077b.tar.gz
```

20多个key。估计是p, q重复使用的问题。

从每个key文件中提取N, e。 对每两个N求gcd，得到p(或q)。可求另一个 q= N/p

之后求fi = (p - 1) * (q - 1)。 de = 1 in fi, 可以求 d.

知道N, e, d, p, q就可以解密了.

```
#!/usr/bin/python
import sys
import gmpy2
from gmpy2 import mpz
import os
import re

from Crypto.PublicKey import RSA
from Crypto.Cipher import PKCS1_OAEP

ns = [0] * 24
es = [0] * 24

for kf in os.listdir('./challenge'):
 match = re.search(r"(\d+).key", kf)
 if not match:
  continue
 f = open(os.path.join('./challenge', kf), 'r')
 key = RSA.importKey(f.read())
 i = int(match.group(1))
 ns[i] = mpz(key.n)
 es[i] = mpz(key.e)
 f.close()

ps = [0] * len(ns)
```

```
qs = [0] * len(ns)
print len(ns)

for i in range(0, len(ns)):
 for j in range(i + 1, len(ns)):
  p = gmpy2.gcd(ns[i], ns[j])
  if p != 1 and gmpy2.is_prime(p):
   ps[i] = p
   ps[j] = p

   qs[i] = gmpy2.t_div(ns[i], p)
   assert gmpy2.is_prime(qs[i]) == True

   qs[j] = gmpy2.t_div(ns[j], p)
   assert gmpy2.is_prime(qs[j]) == True

fis = [0] * len(ns)
ds = [0] * len(ns)
for i in range(0, len(ns)):
 fis[i] = (ps[i] - 1) * (qs[i] - 1)
 ds[i] = gmpy2.invert(es[i], fis[i])

pt = [0] * 24
for kf in os.listdir('./challenge'):
 match = re.search(r"(\d+).enc", kf)
 if not match:
  continue
 i = int(match.group(1))
 f = open(os.path.join('./challenge', kf), 'r')
 key = (long(ns[i]), long(es[i]), long(ds[i]), long(ps[i]), long(qs[i]))
 key = RSA.construct(key)
 cipher = PKCS1_OAEP.new(key)
 pt[i] = cipher.decrypt(f.read())
 f.close()
print ''.join(pt)
```

创作打卡挑战赛

赢取流量/现金/CSDN周边激励大奖